



[READ THE FAQ \(./faq\)](#)

**From the Desk
of Joseph R. Swedish
President and CEO Anthem, Inc.**

To Our Members,

Safeguarding your personal, financial and medical information is one of our top priorities, and because of that, we have state-of-the-art information security systems to protect your data. However, despite our efforts, Anthem was the target of a very sophisticated external cyber attack. These attackers gained unauthorized access to Anthem's IT system and have obtained personal information from our current and former members such as their names, birthdays, medical IDs/social security numbers, street addresses, email addresses and employment information, including income data. Based on what we know now, there is no evidence that credit card or medical information, such as claims, test results or diagnostic codes were targeted or compromised.

Once the attack was discovered, Anthem immediately made every effort to close the security vulnerability, contacted the FBI and began fully cooperating with their investigation. Anthem has also retained Mandiant, one of the world's leading cybersecurity firms, to evaluate our systems and identify solutions based on the evolving landscape.

Anthem's own associates' personal information - including my own - was accessed during this security breach. We join you in your concern and frustration, and I assure you that we are working around the clock to do everything we can to further secure your data.

Anthem will individually notify current and former members whose information has been accessed. We will provide credit monitoring and identity protection services free of charge so that those who have been affected can have peace of mind. We have created a dedicated website - www.AnthemFacts.com (<http://www.AnthemFacts.com>) - where members can access information such as frequent questions and answers. We have also established a dedicated toll-free number that both current and former members can call if they have questions related to this incident. That number is: 1-877-263-7995. As we learn more, we will continually update this website and share that information you.

I want to personally apologize to each of you for what has happened, as I know you expect us to protect your information. We will continue to do everything in our power to make our systems and security processes better and more secure, and hope that we can earn back your trust and confidence in Anthem.

Sincerely,

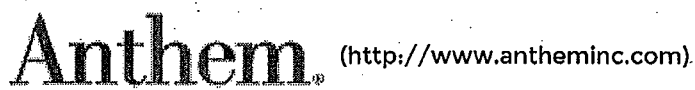
Joseph R. Swedish
President and CEO
Anthem, Inc.

Still have more questions?

READ THE FAQ
(./faq)

©2005-2015 Anthem, Inc. All Rights Reserved: Legal
(<http://www.antheminc.com/Legal/index.htm>) | Privacy
(<http://www.antheminc.com/Privacy/index.htm>)

Updated: 21:25, 02/04/2015



READ THE SPECIAL
MESSAGE FROM JOSEPH
R. SWEDISH (/)

Frequently Asked Questions

**Learn more about the cyber attack
against Anthem**

Was my information accessed?

Anthem is currently conducting an extensive IT Forensic Investigation to determine what members are impacted. We are working around the clock to determine how many people have been impacted and will notify all Anthem members who are impacted through a written communication.

What information has been compromised?

Initial investigation indicates that the member data accessed included names, dates of birth, member ID/ social security numbers, addresses, phone numbers, email addresses and employment information.

Who is responsible for this cyber attack or breach?

Anthem is working closely with federal law enforcement investigators. At this time, no one person or entity has been identified as the attacker.

When will I receive my letter in the mail?

We continue working to identify the members who are impacted. We will begin to mail letters to impacted members in the coming weeks.

How can I sign up for credit monitoring/identity protection services?

All impacted members will receive notice via mail which will advise them of the protections being offered to them as well as any next steps.

Do the people who accessed my information know about my medical history?

No - our investigation to date indicates there was no diagnosis or treatment data exposed.

Do the people who accessed my information have my credit card numbers?

No, our current investigation shows the information accessed did not include credit card numbers.

Did this impact all lines of Anthem Business?

Yes, all product lines are impacted.

Is my (plan/brand) impacted?

The impacted (plan/brand) include Anthem Blue Cross, Anthem Blue Cross and Blue Shield, Blue Cross and Blue Shield of Georgia, Empire Blue Cross and Blue Shield, Amerigroup, Caremore, Unicare, Healthlink, and DeCare.

How can I be sure my personal and health information is safe with Anthem, Inc.?

Anthem is doing everything it can to ensure there is no further vulnerability to its database warehouses. Anthem has contracted with a global company specializing in the investigation and resolution of cyber attacks. We will work with this company to reduce the risk of any further vulnerabilities and work to strengthen security.

©2005-2015 Anthem, Inc. All Rights Reserved.

Legal (<http://www.antheminc.com/Legal/index.htm>) | Privacy
(<http://www.antheminc.com/Privacy/index.htm>)

Updated: 21:25, 02/04/2015

From: Benefits
Sent: Thursday, February 05, 2015 10:13 AM
Subject: IMPORTANT NOTICE: Anthem security breach
Attachments: Anthem Notice.pdf

Dear YP colleague,

Today it was announced that Anthem, Inc., one of the country's largest healthcare providers, has been the victim of a cyber attack and security breach. Their systems were hacked and data on some Anthem subscribers, such as addresses, names, and social security numbers, have been accessed.

Anthem administers YP's medical plans (non-HMOs). This morning, Anthem's president, Joseph Swedish, issued a notice to our YP Benefits Team and its other corporate clients, and we are attaching it to this email for your reference. Here's what we know:

- Once Anthem determined it was the victim of a sophisticated cyber attack, it immediately notified federal law enforcement officials and shared the indicators of compromise with the HITRUST C3 (Cyber Threat Intelligence and Incident Coordination Center).
- Anthem's Information Security has worked to eliminate any further vulnerability and continues to secure all of its data.
- Anthem immediately began a forensic IT investigation to determine the number of impacted consumers and to identify the type of information accessed. The investigation is still taking place.
- The information accessed includes member names, member health ID numbers/Social Security numbers, dates of birth, addresses, telephone numbers, email addresses and employment information, including income data. Social Security numbers were included in only a subset of the universe of consumers that were impacted.
- Anthem is still working to determine which members' Social Security numbers were accessed.
- Anthem's investigation to date shows that no credit card or confidential health information was accessed.
- Anthem has advised us there is no indication at this time that any of our clients' personal information has been misused.
- All impacted Anthem members will be enrolled in identity repair services. In addition, impacted members will be provided information on how to enroll in free credit monitoring.

Anthem has established a website for continuing updates and Q&As for its members: <http://www.AnthemFacts.com>. There you can receive ongoing information from Anthem. We will provide any YP-specific updates as they are received by Anthem.

-- Distributed by YP Benefits. For internal use only. Not to be distributed outside of YP.

From: Benefits
Sent: Wednesday, February 18, 2015 1:17 PM
Subject: UPDATE: Anthem breach

Dear YP Team Members:

Anthem has shared the following update with its corporate clients this week:

In light of the recent security breach, Anthem wants to keep you informed about their actions in response to the cyber-attack. If you have given Anthem your email address, you will get an email this week about identity protection and credit monitoring services. Anthem is **required** to send this email due to state laws around breach notifications. The subject line of the email will be "Important Message From Anthem, Inc." and it will direct you to visit AnthemFacts.com to sign up for credit protection services. All members whose information was in the impacted data warehouse will automatically receive free credit protection services for two years. The email will not ask for personal information and will not reference any other web site. We encourage you to read the email and visit AnthemFacts.com to sign up for the services provided by Anthem.

Member Notification Email FAQ — For Internal Use Only

Is Anthem required to provide email notifications?

Yes, Anthem is required to send emails to members due to state breach notification requirements. Members who have provided e-mails to Anthem and have opted in to receiving communications may receive an email directing them to visit AnthemFacts.com to sign up for credit protection services. The email will not ask for personal information and will not link to any websites other than AnthemFacts.com.

When will member emails be sent?

Emails are planned to begin deploying to over 8 million Anthem current and former members the morning of Wednesday, Feb. 18. We will send 86,000 an hour for the first 2-3 days up to 1 million emails per day. We will then send 1 million a day in one send until complete.

Where will the email come from and what will the subject line be?

The email will be sent from Anthem, Inc. The subject line will be "Important Message From Anthem, Inc."

Can we see a copy of the final email?

A copy of the email will be posted on AnthemFacts.com, and is the exact information in the letters members will receive via U.S. Postal Service. We will also include a link to the email design in the FAQ and group communications so groups can ensure employees know what to look for.

What about Spanish-speaking members?

The email and letter will include a line in Spanish directing members to antheminforma.com.

Si necesita información en español, ingrese en antheminforma.com.

How will the email be branded?

It will be branded Anthem Inc.

Will the email include links?

No links will be coded into the email but there is the possibility that some phones and web platforms will automatically convert the copy into links. We included a sentence to remind members they can key in the web addresses versus clicking directly in the email.

Will those on the Do Not Contact list receive the email?

Yes, since the email is a substitute notice under state breach notification requirements, the Do Not Contact restrictions do not apply. Information regarding this notice was shared with groups on Feb. 13. The only members NOT receiving this email would be those on National DNC registry and those who have unsubscribed.

Can we tell which groups will get the emails on which day?

No, the lists are random and will include all segments (ANA, LG, SG, IND, Medicare, Medicaid), beginning tomorrow night.

Will members of other Blue plans receive a different version?

No, there will be a single version for both Anthem members and members of other blue plans. They will be included toward the back-half of sends. (The approach is being vetted with other Blue plans.)

-- Distributed by YP Benefits. For internal use only. Not to be distributed outside of YP.

From: Benefits
Sent: Tuesday, May 12, 2015 9:35 AM
Subject: ATTENTION: Anthem Security Breach Follow-up

Follow Up Flag: Follow up
Flag Status: Flagged

Dear Team Member,

As you know, on January 5, 2015, Anthem Inc. healthcare company discovered that cyber attackers executed a sophisticated attack to gain unauthorized access to Anthem's IT system and obtained personal information relating to individuals who we or are currently, covered by Anthem. The information accessed may have included YP team members' Social Security numbers and the Social Security numbers of their spouses and dependent children. Anthem believes that this suspicious activity may have occurred over several weeks beginning in early December 2014. Upon discovery of the attack, Anthem began working to close the security vulnerability and contacted the Federal Bureau of Investigation. Anthem has also retained Mandiant, a leading cybersecurity firm, to assist in its investigation. As a company that is an Anthem client, YP strongly encourages its team members to take action to confirm whether or not they may have been impacted by this Anthem breach.

Steps You Can Take To Protect Yourself

Anthem is working with **AllClear ID**, a leading and trusted identity protection provider, to offer 24 months of identity theft repair services to current or former members of an affected Anthem plan. AllClear ID can assist you with identity repair assistance. This service is automatically available to you with no enrollment required. If you experience identity theft, please call them immediately and one of their investigators will assist you to recover financial losses, restore your credit, and make sure your identity is returned to its proper condition.

For additional protection, and at no cost, you may also enroll in the **AllClear PRO** service at any time during the 24 month coverage period. This service includes credit monitoring and an identity theft insurance policy, along with child identity protection. You can enroll at <https://anthem.allclearid.com/> or call AllClear PRO at 877-263-7995 and press 1 to speak with representative. Anthem members who wish to extend their service after the Anthem services expire may do so for \$8.50 per month. An adult can extend their child's service for \$3.95 per month.

If you have additional questions on whether your information was impacted including your Social Security Number, the AllClear phone representative at 877-263-7995 can transfer you over to an Anthem phone representative to verify your information. The Anthem phone representative will ask for your name, your member ID Card number and possibly additional personal information to ensure that we protect your personal health information (PHI). The only thing they can share is whether you were impacted and if so whether your Social Security Number was impacted. Hours of operation for this phone unit are 9 A.M. to 9 PM Eastern Time, Monday through Saturday. **We strongly encourage every team member to call and find out if he/she has been impacted, as well as their covered dependents.**

YP has been assured by Anthem that they are committed to working with each of our team members and providing guidance and assistance related to the cyber-attack.

Credit Bureau Information

You can also obtain information from the Federal Trade Commission and the nationwide credit bureaus about fraud alerts and security freezes. You can add a fraud alert to your credit report file to help protect your credit information. A fraud alert can make it more difficult for someone to fraudulently obtain credit in your name because it alerts creditors to follow certain

procedures to protect you. However, it may also delay your ability to obtain credit. To place a fraud alert in your file, call any one of the credit bureaus listed below. As soon as the credit bureau processes your fraud alert, it will notify the other two credit bureaus, which will also place fraud alerts in your file. In addition, you can visit the credit bureaus at the web address listed below to determine if and how you may place a security freeze on your credit report to prohibit a credit bureau from releasing information from your credit report without your prior written authorization.

- Equifax Security Freeze: https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp
- Experian Security Freeze: http://www.experian.com/consumer/security_freeze.html
- TransUnion Security Freeze: <http://www.transunion.com/personal-credit/credit-disputes/credit-freezes.page>

Equifax 800-685-1111 www.equifax.com P.O. Box 740241 Atlanta, GA 30374-0241	Experian 888-397-3742 www.experian.com P.O. Box 9532 Allen, TX 75013	TransUnion 800-916-8800 www.transunion.com P.O. Box 6790 Fullerton, CA 92834-6790
--	--	---

--Issued by YP Human Resources. For internal use only. Not for distribution outside of YP.